FULL CONTENTS

[Claim(s)]
[Claim 1] An information acquisition means to acquire the privacy information inputted by the user and the 1st information, An information storing means to match the cryptographer stage which enciphers said 1st information, and said 1st information enciphered as said privacy information, and to store in predetermined storage, The privacy information protection system characterized by providing the search means which reads the privacy information which corresponds from said storage based on the 1st information which was inputted into read-out of said privacy information, and was enciphered by said cryptographer stage.
[Claim 2] In the privacy information protection method which stores in predetermined storage the privacy information inputted by the user, and reads said privacy information from said storage according to the directions from a user The privacy information protection method characterized by reading said privacy information based on this 1st information that matched with the 1st information which had privacy information enciphered, stored in said storage, and was enciphered at the time of privacy information read-out.

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the privacy information protection system which secures privacy information safely, and its method.
[0002]
[Description of the Prior Art] In the system which secures individual privacy information conventionally In order to prevent that a user's privacy information is revealed outside, the privacy information which enciphered the privacy information inputted by the user and was

enciphered as identification information was matched mutually, and it stored in storage.

[0003]

[Problem to be solved by the invention] However, in the conventional system mentioned above, since privacy information is enciphered and it is stored in storage, when reading privacy information, the enciphered information must be decrypted and a user must be shown. Therefore, since the decoding processing of information influenced a system throughput fall greatly, there was a problem that information could not be promptly offered to a user.

[0004] This invention was made in view of such a situation, and it aims at offering the privacy information protection system which can offer information quickly to a user, and its method by reading privacy information efficiently, ensuring the safety of privacy information.

[0005]

[Means for solving problem] An information acquisition means to acquire the privacy information as which this invention was inputted by the user in order to attain the above-mentioned purpose, and the 1st information, An information storing means to match the cryptographer stage which enciphers said 1st information, and said 1st information enciphered as said privacy information, and to store in predetermined storage, It is inputted into read-out of said privacy information, and is characterized by providing the search means which reads the privacy information which corresponds from said storage based on the 1st information enciphered by said cryptographer stage.

[0006] According to the above-mentioned composition, match with the 1st information which had the privacy information which is not enciphered enciphered, store in storage, and it sets at the time of privacy information read-out. Since the privacy information which is not enciphered based on this 1st enciphered information is read, it is not necessary to encipher and decrypt privacy information. Thereby, a system throughput fall can be suppressed and management of search key information required for cipher processing also becomes unnecessary.

[0007] Moreover, as for said 1st information, in the above-mentioned privacy information protection system, it is desirable that it is, said user's information about an attribute, i.e., identification information. Thus, it can prevent forgetting key information for a user reading privacy information by making into a user's identification information, including a name, the telephone number, an address, etc., the 1st information which is key information for recognizing privacy information.

[0008] Moreover, this invention offers the method realized by the above-mentioned privacy information protection system.

[0009]

[Mode for carrying out the invention] With reference to Drawings, one embodiment of this invention is explained hereafter. Drawing 1 is the figure showing the system configuration of the privacy information protection system concerning one embodiment of this invention. In this

figure, a sign 1 is an input unit into which a user inputs various information, including privacy information, identification information, etc., and is equipped with the display (illustration abbreviation) which displays the control unit (illustration abbreviation) which inputs information, and information. The hash processor which functions as a cryptographer stage which enciphers the information as which the sign 2 was inputted, The coupler which functions as an information storing means for a sign 3 to match the information by which hash processing was carried out with the hash processor 2, and the information by which hash processing is not carried out, and to store in the storage 4, A sign 5 is a retrieval device which reads the information which was inputted into read-out of privacy information from the input unit 1, and was enciphered by the hash processor 2, for example, the privacy information which corresponds from the storage 4 based on identification information. In addition, as long as the storage 4 has the function to store information and there is, the thing of what kind of form is sufficient as it. In addition, the privacy information protection system concerning this embodiment consists of the input unit 1, a hash processor 2, a coupler 3, and a retrieval device 5.

[0010] Next, operation of the privacy information protection system which consists of the above-mentioned composition is explained. First, a user inputs into self identification information (identification information is called hereafter) and others the privacy information which is information to make secret from the input unit 1. If identification information and privacy information are inputted by the user, the input unit 1 will output identification information to the hash processor 2, and will output privacy information to the coupler 3.

[0011] The identification information inputted into the hash processor 2 is outputted to the coupler 3, after hash processing is carried out. The coupler 3 combines the privacy information inputted without minding the identification information and the hash processor 2 by which hash processing was carried out, and stores it in the storage 4 by making this information into connected information. If it puts in another way, the coupler 3 matches mutually the identification information enciphered by carrying out hash processing, and the privacy information which is not enciphered, and stores it in the storage 4. As a result, the hash information and privacy information of identification information which were matched mutually are stored in the storage 4.

[0012] Next, a user inputs the identification information used as the key of privacy information search to read the self privacy information stored in the storage 4, after operating the purport of data read from the input unit 1. The inputted identification information is outputted to the hash processor 2 from the input unit 1, and hash processing is carried out here and it is outputted to the retrieval device 5 after that. The retrieval device 5 reads the privacy information which is matched and is stored in this identification information from the inside of the storage 5 by using as a search key the identification information by which hash processing

was carried out, and outputs this privacy information to the input unit 1. Thereby, a user's privacy information is displayed on the display screen of the input unit 1. In addition, it may be performed by the case where the output from the input unit 1 to the hash processor 2 is performed automatically, and directions of a user.

[0013] As mentioned above, according to the privacy information protection system concerning this embodiment, the identification information which is a search key is enciphered (hash processing), but privacy information is not enciphered. Therefore, in the case of privacy information read-out, it becomes unnecessary to decrypt privacy information and a system throughput fall can be controlled.

[0014] As mentioned above, although the embodiment of this invention has been explained in full detail with reference to Drawings, concrete composition is not restricted to this embodiment and the design of the range which does not deviate from the summary of this invention etc. is included.

[0015]

[Effect of the Invention] [according to the privacy information protection system of this invention] as explained above Match with the 1st information which had the privacy information which is not enciphered enciphered, store in storage, and it sets at the time of privacy information read-out. Since the privacy information which is not enciphered based on the 1st enciphered information is read and it is not necessary to encipher and decrypt privacy information, a system throughput fall can be suppressed. Thereby, although the safety of privacy information is ensured, it becomes possible to perform writing and read-out of privacy information efficiently, and the effect that information can be quickly offered to a user is done so.
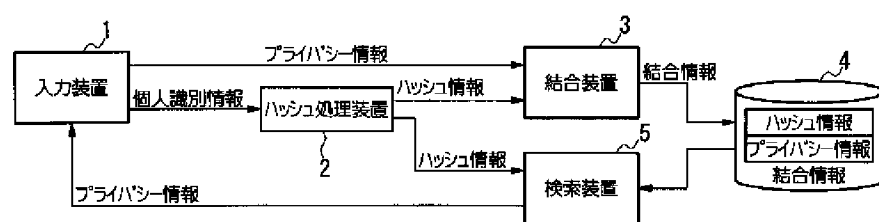

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the system configuration of the privacy information protection system concerning one embodiment of this invention.
[Explanations of letters or numerals]
1 [-- Storage, 5 / -- Retrieval device] -- An input unit, 2 -- A hash processor, 3 -- A coupler, 4

[Drawing 1]

入力装置 1 ──プライバシー情報──→ 結合装置 3 ──結合情報──→
入力装置 ──個人識別情報──→ ハッシュ処理装置 2 ──ハッシュ情報──→ 結合装置
ハッシュ処理装置 ──ハッシュ情報──→ 検索装置 5
──プライバシー情報──→

4
ハッシュ情報
プライバシー情報
結合情報

[Translation done.]